Implications of Firmware Trickery in Metamorphic Hard Drives

Courtney Webb
@courtneyjjjwebb
thatharddriveguy@gmail.com

SANS #DFIRSummit
Austin, TX
June 2017
WHO AM I?

- DF Team Leader in Australia [Oz-stray-yaaaah]
- Law Enforcement for 12 years
- Hardware tinkerer
- Researching Forensics and Data Recovery

Image by Cheeky4n6Monkey
cheeky4n6monkey.blogspot.com
BEGINNING

- HDDHackr source code released
- Research into ATA commands
- Deconstruct Firmware data
- Forensic and DR knowledge
- Media articles similar ideas
METAMORPHIC?

- Alter HDD identity
- Restrict area
- Hide ‘badness’
- Not HPA or DCO
- Manipulate HDD firmware
FIRMWARE

- Embedded system
- Small computer in bigger computer???
- Boot code
- Unique parameters
- Identification data
- ‘Precisely’ 2.5 locations
System Area
RECOVERY
ALTERATION

- **Vendor Specific Commands**
- VSC used to alter SA, ROM, RAM through:
- normal SATA/PATA
  OR
  Serial (RS232 adapter)
- QA/Calibration/Diagnostics
VSC SECURITY

- “Only known to Manufacturer”
- “Just costly professional tools”
- “People willing to spend money”
- 2 out of 3 manufacturers VSCs easily known
- Represent 80% HDD market
This presentation is not intended to:

- Name/shame the manufacturer
- Provide a walkthrough
- Disclose any intellectual property
NON-DISCLOSURE

- It is intended to highlight the:
  - Ease it could be done
  - Implications and risks
  - Possible solutions/improvements
Analogous fictional manufacturer rather than Toshiba, Seagate or Western Digital

Called 'Southern Analogue'

Perform two alterations;

- Exterior appearance
- Interior identification
EXTERIOR
REVEAL
VSC will piggyback on ATA committee standard commands (SMART Command Transport)

SMART WRITE LOG and SMART READ LOG

Need to tell drive to look for these commands

Use a Super ON command

registers = BE EF 00 41 53 a0 80

Proprietary ASCII INITIALS
Send a SMART WRITE LOG command with the VSC as the 'log data'

registers = d6 c0 de 4f c2 a0 b0

Proprietary

- VSC is ~3-16 bytes long
- Contained in a 512 byte sector padded with zeroes
Send a SMART READ LOG command

The requested module is returned

registers = d5 fa ce 4f c2 a0 b0

Proprietary
- MHDD program used
- Boot off USB
- Simple scripting language
- Can use notepad
- Hex editor for VSC file

```plaintext
; read config sector
reset
waitnbsy
regs = $BE $EF $00 $41 $53 $a0 $80
waitnbsy
regs = $d6 $** $** $4f $c2 $a0 $b0
waitnbsy
cHECKDR
sectorsfrom = VSC.bin

regs = $d5 $** $** $4f $c2 $a0 $b0
waitnbsy
cHECKDR
sectorssto = CONFIG.bin

; end
```
MHDD

MHDD> write
MHDD ATA/SCSI TERMINAL v2.1
Script: WRITE0D

LINE 1: RESET
LINE 2: WAITMSY
LINE 3: REGS = $30 $AO $80
LINE 4: WAITMSY
LINE 5: REGS = $D6 $4F $CZ $AO $BO
LINE 6: WAITMSY
LINE 7: CHECKDRQ
LINE 8: SECTORSFROM = WRT_0D.BIN
LINE 9: WAITMSY
LINE 10: REGS = $D5 $4F $CZ $AO $BO
LINE 11: WAITMSY
LINE 12: CHECKDRQ
LINE 13: SECTORSFROM = MOD0D.BIN

All done.
MHDD>

I Select a drive : <SHIFT+F3>
Implications

- Indistinguishable drive
- Hide data from:
  - Forensic Tools,
  - Operating Systems
  - Data Recovery Tools
- How many have we missed?
- Great for infiltration or exfiltration
<table>
<thead>
<tr>
<th>Software</th>
<th>Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>MHDD</td>
<td>DFL-ST &amp; DFL-WD</td>
</tr>
<tr>
<td>WDR</td>
<td>Salvation Data Disk Doctor</td>
</tr>
<tr>
<td>WD Marvel</td>
<td>MRT</td>
</tr>
<tr>
<td>SeDiv</td>
<td>HRT</td>
</tr>
<tr>
<td>HDDSuperTool</td>
<td>DeepSpar Disk Imager</td>
</tr>
<tr>
<td>Nayzura</td>
<td>Atola Insight</td>
</tr>
<tr>
<td>ST Mem</td>
<td>PC3000</td>
</tr>
<tr>
<td>HDDHACKKR</td>
<td></td>
</tr>
</tbody>
</table>
Search for Artefacts scripts and data files

Suspicious drives subjected to deep interrogation

Compare internals to matching drive
FORENSICS

Copy all Firmware → Inspect Firmware

Attempt to Change Size ← Compare to Internals
PROBLEMS

Physically Identical Drives

Refurbished Drives
SOLUTIONS

- Known Good FW Samples
- Internal Integrity Validation
- Trusted Platform Model
<table>
<thead>
<tr>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command to write to physical sectors or unused sectors (PCHS)</strong></td>
</tr>
<tr>
<td>POC tool used to write to unused area of system area</td>
</tr>
<tr>
<td>Mark spare 1TB of disk as part of the system area</td>
</tr>
<tr>
<td>Write/read directly to that area</td>
</tr>
<tr>
<td>Explore possibilities with Solid State Drives</td>
</tr>
</tbody>
</table>
QUESTIONS?

Twitter: @courtneyjjjwebb
Email: thatharddriveguy@gmail.com